
دار المنظومة
DAR ALMANDUMAH
الرواد في قواعد المعلومات العربية

الجهود الدولية في مكافحة الجرائم المعلوماتية والصعوبات التي تواجها

وائل محمد نصيرات

كلية الإدارة والأعمال، قسم الأنظمة، الإدارة القانونية

جامعة الأميرة نورة بنت عبد الرحمن

الرياض، السعودية

Wael_a٧٣@yahoo.com

الملخص – تتناول ورقة البحث المقدمة إلى المؤتمر الدولي الأول حول "مكافحة الجرائم المعلوماتية" موضوع (الجهود الدولية في مكافحة الجرائم المعلوماتية والصعوبات التي تواجها) حيث تعد الجرائم المعلوماتية من أخطر الجرائم التي ظهرت في العصر الحديث والتي تؤثر سلبا على الفرد والمجتمع وكذلك على الصعيد الدولي لأنها تنمو متطور ومستمر اطرادا مع نمو عصابات الجريمة المعلوماتية كما يثير خطر جرائم المعلوماتية، وأهمية مكافحتها اهتماما كبيراً لدى الرأي العام المحلي، والدولي، بالنسبة لآثاره الاجتماعية والمالية والاقتصادية والأمنية.

١. تمهيد

الحمد لله رب العالمين، والصلاة والسلام على أشرف الأنبياء والمرسلين، نبينا محمد وعلى آله وصحبه أجمعين، أما بعد، مع دخول الحاسوب والإنترنت إلى مجتمعاتنا وفي كافة جوانب حياتنا بدأً يظهر نوع جديد من الجرائم تسمي الجرائم المعلوماتية وبالتالي أصبح هناك حاجة لتعريف هذه الجرائم والتوعية ومتابعة هذا النوع من الجرائم وسن القوانين والتشريعات اللازمة لمكافحة الجرائم الإلكترونية نظراً لما تسببه من خسائر مادية ومعنوية كبيرة.

لقد باتت الجرائم المعلوماتية خطراً يهدد أمن المجتمعات وأخلاقها ومكتسباتها، الأمر الذي دفع بالمجتمع الدولي إلى البحث عن آليات جديدة تتلاءم وطبيعتها، وتطوير الوسائل التقليدية بما يكفل تضامن جهول الدول، وأجهزتها القائمة بمهمة مكافحة الجرائم المعلوماتية [1]. وقد اقتضي البحث في مسألة الجهود الدولية في مكافحة الجرائم المعلوماتية والصعوبات التي تواجها أن يكون في مقدمة، ومبحثين، وخاتمة، على النحو الآتي:

المبحث الأول: الجهود الدولية والإقليمية لمكافحة جرائم المعلوماتية

المطلب الأول: الجهود الدولية لمكافحة جرائم المعلوماتية

المطلب الثاني: الجهود الإقليمية لمكافحة جرائم المعلوماتية.

المبحث الثاني: الصعوبات التي تواجه الجهود الدولي لمكافحة جرائم المعلوماتية.

المبحث الثاني: الصعوبات التي تواجه الجهود الدولي لمكافحة جرائم المعلوماتية وكيفية القضاء عليها.

المطلب الأول: الصعوبات التي تواجه الجهود الدولية لمكافحة جرائم المعلوماتية.

المطلب الثاني: كيفية القضاء على الصعوبات التي تواجه الجهود الدولية في مكافحة جرائم المعلوماتية.

٢. أهمية الدراسة

تكمن أهمية الدراسة في السعي وراء المحاولة والتقصي لإيجاد واستنباط بعض الحلول والمقترحات الممكنة لمكافحة الجرائم المعلوماتية بوصفها جرائم مرتبطة بالثورة والمعرفة المعلوماتية ونظرا لخطورتها ومدى انتشارها فإنه يلزم تدخل المشرع واحتوائها في نصوص قانونية تشمل التجريم والعقاب، وبيان الدور الذي تلعبه التشريعات الداخلية والاتفاقات الدولية في مكافحتها والحد منها ومنع تفشيها.

٣. أهداف الدراسة

١. التعرف على الجهود المبذولة في مواجهة الجرائم المعلوماتية.

٢. بيان الصعوبات التي تواجه الجهود الدولية في القضاء على الجرائم المعلوماتية.

٣. التعمق في الوسائل الممكنة للقضاء على الجريمة المعلوماتية.

٤. تساؤلات الدراسة

وسوف تحاول هذه الورقة الإجابة على الأسئلة الآتية:

١. ما هي الجهود المبذولة في مواجهة الجرائم المعلوماتية؟

٢. ما الصعوبات التي تواجه الجهود الدولية في القضاء على الجرائم المعلوماتية؟

٣. ما هي الوسائل الممكنة للقضاء على الجريمة المعلوماتي؟

٥. مفاهيم الدراسة

- الجريمة المعلوماتية: أي فعل يرتكب متضمناً استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخافة لأحكام هذا النظام.
- الموقع الإلكتروني: مكان إتاحة البيانات على الشبكة المعلوماتية من خلال عنوان محدد.
- شبكة المعلوماتية: ارتباط بين أكثر من حاسب آلي أو نظام معلوماتي للحصول على البيانات وتبادلها، مثل الشبكات الخاصة والعامة والشبكة العالمية.

٦. منهج الدراسة

كون هذا الدراسة تتناول الجهود الدولية في مكافحة الجرائم المعلوماتية والصعوبات التي تواجها فإن المنهج العلمي المتبع فيها سيكون المنهج الوصفي التحليلي المقارن إذ سأتعرض للجهود الدولية والإقليمية لمكافحة جرائم المعلوماتية، كما نتناول النصوص النظامية لمحاولة الإجابة عن إشكالية الدراسة وتحليلها ووضع الحلول المناسبة من أجل الوصول إلى الهدف من الدراسة المتمثل في معرفة كيفية القضاء على الصعوبات التي تواجه الجهود الدولية في مكافحة جرائم المعلوماتية.

٧. محددات الدراسة

ولما كان الموضوع الذي تدور حوله دراستنا هو الجهود الدولية في مكافحة الجرائم المعلوماتية والصعوبات التي تواجها فإننا لن نستعرض الجهود الدولية الإقليمية لمكافحة جرائم المعلوماتية، بل سنركز على جهود بعض الدول العربية لمكافحة جرائم المعلوماتية مع بيان المعوقات التي تواجها.

المبحث الأول

الجهود الدولية والإقليمية لمكافحة جرائم المعلوماتية

إن مكافحة الجرائم المرتبطة بتكنولوجيا المعلوميات التي باتت في مظهرها وتجلياتها الحديثة لن تكون مجدية إلا إذا كان هناك تعاون وتآزر دوليين على أكبر قدر من التنسيق [٢]. ومن هنا بدأت بعض الأصوات ترتفع للمطالبة بضرورة سن قوانين لحماية المعلومات على الشبكات، بالإضافة إلى إدراك الدول والحكومات حجم المخاطر التي تزداد معها جرائم الإنترنيت، فأنشئت جهات رسمية لمكافحة هذه الجرائم وسنت قوانين لحماية شبكة المعلومات. بالإضافة إلى أن وعي هذه الدول بمدي خطورة هذه الجرائم العابرة للحدود كان نتيجة لإبرام عدة اتفاقيات ومعاهدات دولية، في مجال مكافحة هذه الجرائم التي باتت تهددها خاصة مع ازدياد استعمال التكنولوجيا الحديثة يوما بعد يوم.

المطلب الأول: الجهود الدولية لمكافحة جرائم المعلوماتية..

أولا: الاتفاقية الأوربية لمكافحة جرائم الإنترنيت ومعاهده بودابست/ ٢٠٠١.

تعتبر كل من معاهدة بودابيست والمعاهدة الأوربية من أهم المعاهدات التي أبرمت لمكافحة جرائم الأنترنيت في إطار التعاون الدولي.

- معاهدة بودابيست لمكافحة جرائم الإنترنيت.

فقد تم توقيع هذه المعاهدة في بودابستت ٢٠٠١ اقتناعا من المجلس بأن هذه الاتفاقية ستوفر ما يلزم لردع أي عمل موجه ضد السرية والنزاهة وتوفر نظم الحاسوب والشبكات والبيانات واتخاذ ما يكفي من الإجراءات والصلاحيات لمكافحة هذه الجرائم.

١. أكدت هذه المعاهدة على الحاجة لاتخاذ تدابير تشريعية لمكافحة جرائم المعلوماتية ومخاطرها على الدول والدعوة إلى مكافحة كافة الأنشطة الإجرامية التي تستهدف أمن المعلومات كما تكفل للحكومات حق المراقبة وتلزم الدول بمساعدة بعضها البعض في جمع الأدلة

٢. أيضا أكدت على اتخاذ التدابير التشريعية والتنظيمية لضمان ملاحقة مرتكبي هذه الجرائم وكشفها وتوفير قواعد ملائمة للتحري والتحقيق والضبط والتفتيش والمحاكمة مع التركيز على أهمية التعاون المحلي والإقليمي والدولي. وتوحيد الجهود الدولية في مجال مكافحة جرائم الإنترنيت.

- أما المعاهدة الأوروبية لمكافحة جرائم الأنترنيت [٣].

فقد ستلزمت الدول الموقعة عليها بسن الحد الأدنى من القوانين الضرورية للتعامل مع جرائم التقنية العالية بما في ذلك الدخول غير المصرح به إلى شبكة ما والتلاعب بالبيانات وجرائم الاحتيال والتزوير التي لها صلة بالكومبيوتر وصور القاصرين الإباحية وانتهاكات حقوق النسخ الرقمي.

ثانياً: الاتفاقية الأمريكية المتعلقة بجرائم الحاسب الآلي والإنترنيت لسنة ١٩٩٩

عقد في جامعة ستانفورد في ولاية كالفيورنيا في الولايات المتحدة مؤتمر للفترة من ٦ – ٧ ديسمبر ١٩٩٩ بمشاركة العديد من الهيئات والمنظمات الدولة والممثلين القانونيين [٤].

١. أوجبت هذه الاتفاقية تبني معايير موحدة لمواجهة هذه الجرائم وفرض عقوبات تتناسب مع درجة خطورتها

٢. أيضا بينت الجرائم المعلوماتية وهي التوصيل غير المصرح به وتعديل وحذف البيانات بهدف الإضرار بالمؤسسات التي تملك هذه الخدمات أو حذف البيانات بتغييرها لإعطاء معلومات كاذبة.

٣. أيضا أوضحت أحكام المحاولة أو المساعدة والتحريض والأغراء والتأمر على ارتكاب الجريمة المعلوماتية وكذلك بينت هذه الاتفاقية أحكام اختصاص الولايات الأعضاء في اتخاذ الإجراءات القانونية الملائمة.

المطلب الثاني: الجهود الإقليمية لمكافحة جرائم المعلوماتية.

الفرع الأول: جهود بعض الدول الأجنبية لمكافحة جرائم المعلوماتية.

أولاً: الولايات المتحدة الأمريكية

حيث يشير التقرير الصادر عن وزارة العدل الأمريكية عام ١٩٨٦ إلى أن البنوك الأمريكية تكبده خسائر جسمية خلال السنوات الخمس السابقة لعام ١٩٨٦ من جراء ١٣٩ حالة من حالات الاحتيال والخطأ وقعت أثناء التعاملات التي أجريت عبر الوسائل الإلكترونية لتمويل الاعتمادات والأموال، مرد الخسارة هو الاحتيال للاستيلاء على المال [٥].

وفي دراستين أجرت في الولايات المتحدة عام ١٩٨١، ١٩٨٤ شملت أولاهما: (٧٧) حالة احتيال بواسطة الحاسوب للاستيلاء على المال. وشملت الثانية: (٦٧) حالة من نفس النوع، تبين أن (٥٢)% و(٤٢)% من مجموع حالات كل دراسة على التوالي قد اكتشفت عن طريق الرقابة الداخلية وأن (١٢)% و(٦)% من حالات كل منها على التوالي اكتشفت عن طريق التدقيق الداخلي. وأمام ذلك صدرت في الولايات المتحدة الأمريكية عدة قوانين وتشريعات خاصة للتصدي لبعض الجرائم المعلوماتية ومن أهمها قانون الخصوصية والحقوق الأسرية والتعليمية الصادر عام ١٩٧٤، وقانون سياسة الاتصالات السلكية واللاسلكية لعام ١٩٨٤ والذي يستهدف حماية خصوصية المشتركين في الخدمة التليفونية عبر الإنترنت. أما قانون العقوبات الأمريكي فقد كان من أسبق التشريعات التي تعرضت للجرائم المعلوماتية. ويمكن القول أن الولايات المتحدة الأمريكية قد استكملت بنيتها التشريعية مع نهاية القرن العشرين في

شأن التشريعات التي تحكم المعاملات الإلكترونية وتواجه الجريمة المعلوماتية سواء في تشريعاتها المحلية علي مستوى الولايات أم الاتحادية على مستوى الدولة الفيدرالية ولعل أحدث هذه التشريعات هو قانون التوقيع الإلكتروني الصادر عام ٢٠٠٠ [٦].

ثانياً: المملكة المتحدة

تعد بريطانيا الدولة الثانية في حجم الخسائر أتي تلحقها جرائم الكمبيوتر بعد الولايات المتحدة، وتظهر دراسة نشرها الدكتور [٧] (Ken wong) في المملكة المتحدة عام ١٩٨٦ والتي شملت ١٩٥ حالة احتيال أوغش الحاسوب للاستيلاء على المال النتائج التالية:-

- ١٥% من هذه الحالات اكتشفت نتيجة وعي ودقة الإدارة ومهارتها في الرقابة علي الإجراءات الكتابية واستعمال أساليب الرقابة علي التصنيفات.
- ١٠% منها اكتشفت بناء على شكاوي قدمها المجني عليهم.
- ٧% اكتشف جراء تغييرات في الإدارة نتيجة برمجة التطبيقات لتلائم أجهزة وأنظمة معلوماتية جديدة.
- ١٥% منها اكتشف بمحض الصدفة
- ١٥% منها اكتشف نتيجة معلومات سرية للشرطة ولرب العمل الذي يعمل لديه الفاعل.

وعلى الرغم بعدم توجد تشريعات مكتوبة تعالج ظاهرة الجرائم المعلوماتية، وذلك بسبب كون النظام القانوني الإنجليزي يعتمد على السوابق القضائية المملكة المتحدة، غير أنه في ٢٩ يونيو ١٩٩٠ صدر قانون إساءة استخدام الكومبيوتر في المملكة المتحدة لبيان الجرائم المتصلة بالكومبيوتر وفرض العقوبات المناسبة على مرتكبيها [٨].

ثالثاً: فرنسا

تتعدد في فرنسا القواعد التشريعية التي تخضع لها الجريمة المعلوماتية في القانون الفرنسي، فهذا النمط من الجرائم تحكمه قواعد قانونية أعلى قيمة من القواعد القانونية في القانون الفرنسي تتمثل بقواعد بالوقت الذي عالج فيه قانون العقوبات الفرنسي الجديد رقم (٦٠) الصادر في القانون الأوربي ١٦/ ديسمبر ١٩٩٢ الجرائم المعلوماتية بنصوص مستقلة في الفصل الثاني.

رابعاً: اليابان

في اليابان صدر قانون حظر الدخول للكمبيوتر رقم (١٢٨) والذي بدأ تنفيذه في ٣ فبراير ٢٠٠٠ حيث جرم في المادة (٣) أي فعل للدخول المحظور في الكمبيوتراما المادة (٤) فقد جرمت أي فعل من شأنه تسهيل الدخول المحظور للكمبيوتر. أما المادة (٨ و٩) فقد تضمنت العقوبات [٩].

الفرع الثاني: جهود بعض الدول العربية لمكافحة جرائم المعلوماتية.

أولاً: جهود المملكة العربية السعودي لمكافحة جرائم المعلوماتية.

تحتل المملكة الترتيب الخامس على المستوى العالمي من حيث معدل نمو عدد أجهزة الحاسب الآلي المستخدمة، وهي أكبر أسواق منطقة الشرق الأوسط في أعداد الأجهزة المباعة. ويتجاوز عدد مشتركي الإنترنت ٦٠٠ ألف مشترك كما تم تسجيل أكثر من ٤٥٠٠ اسم نطاق بالمملكة. وتقدر نسبة النمو في قطاع الإنترنت بالسوق السعودي وأكثر من ٢٧٥% [١٠]. كما تعتبر المملكة من الدول التي ترتفع فيها نسبة استخدام البرامج غير المرخصة، وإن كانت الدولة تسعي في الآونة الأخيرة وبشكل حثيث للتصدي لهذه الظاهرة، وقد صدر عن سمو ولي العهد توجيهاً صريحاً للجهات الحكومية بالاعتماد على النسخ الأصلية للبرامج المستخدمة. أيضاً تحتلت المملكة العربية السعودية المركز السادس عالميا بين الدول التي تنطلق منها الهجمات الإلكترونية نسبة إلى عدد مستخدمي الإنترنيت في البلاد [١١]. كما سبقت المملكة العربية السعودية نظيراتها من الدول العربية في إصدار قانون جديد لمكافحة جرائم المعلوماتية فقد صدر نظام مكافحة جرائم المعلوماتية السعودي بالمرسوم ملكي رقم م/ ١٧ بتاريخ ٨/٣/ ١٤٢٨هـ، تضمن تعريف وتحديد الجرائم المعلوماتية والحد منها ومواجهتها بعد أن أصبحت تهدد أمن وسلامة المجتمعات الإنسانية.

١. ما يشتمل عليه نظام مكافحة جرائم المعلوماتية

يشمل هذا النظام (١٦) مادة تتضمن عقوبات صارمة ضد مرتكبي هذه الجرائم تتراوح بين سنة و١٠ سنوات سجنا وغرامات مالية تصل إلى خمسة ملايين ريال سعودي، مضيفاً أن النظام تضمن تعريفات المصطلحات والمسميات الواردة في النظام مثل و"النظام المعلوماتي" و"الشبكة المعلوماتية" و"البيانات والجريمة المعلوماتية إلى جانب أهداف النظام بالحد من هذه الجرائم والعقوبات المقررة لكل منها، وحددت مواد النظام الأخرى الجرائم المعلوماتية وعقوباتها التي تنوعت بين السجن لمدد مختلفة والغرامات المالية بحسب نوع وطبيعة كل جريمة من الجرائم المعلوماتية واختصاصات كل من "هيئة الاتصالات وتقنية المعلومات" و"هيئة التحقيق والادعاء العام" في المساندة اللازمة للأجهزة الأمنية لتحقيق أهداف وغايات هذا النظام.

٢. أهداف نظام مكافحة جرائم تقنية المعلومات.

- إرساء قواعد نظامية موحدة لاستخدام التعاملات والتوقيعات الإلكترونية، وتسهيل تطبيقها في القطاعين العام والخاص بوساطة سجلات الكترونية يعول عليها إضفاء الثقة في صحة التعاملات والتوقيعات والسجلات الإلكترونية وسلامتها.
- تيسير استخدام التعاملات والتوقيعات الإلكترونية على الصعيدين المحلي والدولي للاستفادة منها في جميع المجالات، كالإجراءات الحكومية والتجارة والطب والتعليم وادفع المالي الإلكتروني.
- إزالة العوائق أمام استخدام التعاملات الإلكترونية.
- منع إساءة الاستخدام والاحتيال في التعاملات والتوقيعات الإلكترونية".

٣. الخطوط العامة للمسئولية عن جرائم المعلوماتية

أورد نظام مكافحة جرائم المعلوماتية من النصوص ما يبين الخطوط العامة للمسئولية عن جرائم المعلوماتية وخاصة فيما أورده من أحكام موضوعية للمسئولية الجنائية عن جرائم المعلوماتية على الوجه التالي:

- تقرير عقوبة السجن دون وضع حد أدني لها: يقرر النظام عقوبة السجن للجرائم المعلوماتية دون أن يضع حد أدني لتلك العقوبة. ويلاحظ أن الأنظمة السعودية لم تضع حكما عاما بعقوبة السجن يبين الحد الأدنى لتلك العقوبة، لذا فإنه لا يقل عن يوم واحد.
- الجمع بين عقوبات أصلية وعقوبات تكميلية: يجمع نظام مكافحة جرائم المعلوماتية بين عقوبات أصلية وعقوبات تكميلية. من ناحية العقوبات الأصلية قرر النظام عقوبة السجن وقرر عقوبة الغرامة مع السجن حوارية للمحكمة بقوله "أو بإحدى هاتين العقوبتين". كما أجاز للمحكمة أن تحكم بالغرام بالإضافة إلى السجن؛ عندئذ تصح الغرامة عقوبة تكميلية للسجن. مثال ذلك المادة الرابعة من النظام التي تنص على أنه يعاقب بالسجن مدة لا تزيد على ثلاث سنوات وبغرام لا تزيد على مليوني ريال أو بأحدي هاتين العقوبتين كل شخص يرتكب أيا من الجرائم المعلوماتية الآتية:
- التخيير بين عقوبة الغرامة وعقوبة السجن
- تقرير المصادرة كعقوبة تكميلية جوازية

ثانياً: جهود دولة الإمارات العربية المتحدة لمكافحة جرائم المعلوماتية.

تعتبر دولة الإمارات العربية المتحدة من الدول العربية التي يحظر هذا النوع من الجرائم باعتبارها جرائم حديثة، فقد أصدرت القانون الاتحادي رقم ٢ لسنة ٢٠٠٦ وهو بحق من القوانين الريادية الأولي في العالم العربي الذي تضمن تفاصيل كثيرة وتعد الإمارات العربية المتحدة سباقة في الإسهام بوضع تصورات لمكافحة كل أشكال الجرائم المستحدثة من خلال:

١- مشاركاتها واحتضانها للمؤتمرات والاجتماعات ذات الصلة بهذه الجرائم، مما عكس ذلك جليا بتبني جامعة الدول العربية القانون الاتحادي رقم ٢ لسنة ٢٠٠٦ بشأن مكافحة جرائم تقنية المعلومات كقانون استرشادي.

٢- التركيز على الجانب الوقائي في مكافحة الجريمة وإقرار الأمن والاستقرار والسلامة العامة بين المواطنين والمقيمين على أرض الدولة مع التسلح بالخبرات اللازمة، وإنشاء إدارة الأدلة الإلكترونية ونظام الشرطي الإلكتروني وتدريب الكوادر الفنية للتصدي لهذا النوع من الجرائم عند وقوعها.

٣- تدريب الشرطة من أجل التعامل مع هذه السلوكيات.

٤- كما قامت بدراسات متواصلة فيما يتعلق بالمواقع الإلكترونية، فقد تم الاتفاق بين مدير القنوات الإلكترونية في بنك دبي الإسلامي مع الخبير في أمن المعلومات غسان عايش أن فرقا متخصصة تعمل على مدار الساعة، وتجري البحوث اللازمة لمعرفة الثغرات وأغلاقها قبل وصول المحتالين وقراصنة الإنترنيت لها، بما يؤدي في النهاية إلى حماية العملاء وضمان المعاملات المصرفية الإلكترونية بصورة آمنة (١٢).

- جهود المملكة الأردنية الهاشمية لمكافحة جرائم المعلوماتية

يتمثل دور الأردن في مكافحة جرائم تقنية المعلومات في التشريعات الوطنية، والمستوى الدولي، والمؤسسات الأردنية المعنية بمكافحة الجرائم المعلوماتية، فمن التشريعات الوطنية.

١. قانون المعاملات الإلكترونية رقم (٨٥) لسنة (٢٠٠١) والذي بدأ العمل به في ١/٣/ ٢٠٠١م. ويهدف إلى تنظيم المعاملات التي تتم عبر الوسائل الإلكترونية مع ضرورة مراعاة العرف التجاري الدولي الخاص بها، وتسري أحكام هذا القانون على المعاملات والسجلات والتواقيع الإلكترونية وأية معاملة تتم عبر الوسائل الإلكترونية.

٢. قانون جرائم أنظمة المعلومات رقم (٣٠) لسنة (٢٠١٠) والذي تولي بيان المقصود بالبيانات والمعلومات الإلكترونية وبين أوجه المخالفات التي تشكل جرائم يمكن المعاقبة عليها.

٣. قانون الاتصالات رقم (١٣) لسنة (١٩٩٥) ويعتبر من أول التشريعات التي تناولت ملاحقة مركتبي الجرائم المعلوماتية.

وعلى المستوى الدولي لم تدخر الأردن جهداً في مد أواصر التعاون مع العالم أيضا لغايات مكافحة الجريمة العابرة للحدود، ذلك أنه إذا ما أيقنا أن الجريمة المعلوماتية تعتبر من الجرائم التي يمكن ارتكابها عن بعد وتكون عابرة للحدود، فإنه لابد من وجود تواصل عالمي لملاحقة مرتكبيها والحد من خطورتهم، فقد تم عقد مجموعة من المؤتمرات في الأردن لغاية مناقشة آثار الجريمة المعلوماتية وطرح التوصيات والأفكار حوله (١٣). وفي الأردن يعمل محاموها على مواكبة التطور والاختصاص في مجال المعلوماتيكما صادقت الأردن وتونس علي اتفاقية تسمح بإمكانية استخدام التوقيع الإلكتروني مما يفتح آفاق واسعة أمام معاملات الكترونية جديدة.

التشريع العماني

صدر في سلطنة عمان تشريع خاص بجرائم الحاسب الألي، حيث عاقب المادة (٢٧٦) على أفعال الالتقاط غير المشروع للمعلومات وإتلاف وتغيير ومحو المعلومات وتسريب المعلومات وانتهاك خصوصيات الغير.. الخ. في حين عاقبت المادة (٢٧٦) مكررا كل من استولي على بيانات تخص الغير بطريقة غير مشروعة. وعاقبت المادة (٢٧٦) مكرر ٣ كل من قام بتقليد أو تزوير بطاقات السحب أو استعمال أو حاول استعمال البطاقة المزورة أو المقلدة مع علمه بذلك.

المبحث الثاني

الصعوبات التي تواجه الجهود الدولي لمكافحة جرائم المعلوماتية وكيفية القضاء عليها.

التعاون الدولي بكافة صورة في مجال مكافحة ومواجهة الجرائم المتعلقة بشبكة الإنترنت وإن كان يعد مطلبا تسعي إلى تحقيقه أغلب الدول، إلا أنه ثمة صعوبات ومعوقات تقف دون تحقيقه أهمها:

المطلب الأول: الصعوبات التي تواجه الجهود الدولية لمكافحة جرائم المعلوماتية

الفرع الأول: الصعوبات التشريعية والقضائية التي تواجه الجهود الدولية

أولا: الصعوبات المتعلقة بالمساعدات القضائية الدولية تعرف المساعدة القضائية الدولية بأنها "كل إجراء قضائي تقوم به دولة من شأنه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم" (١٤). وتعد طلبات الإنابة القضائية الدولية من أهم صور المساعدات القضائية الدولية في المجال الجنائي أن تسلم بالطريق الدبلوماسية وهذا بالطبع يجعلها تتسم بالبطء والتعقيد، والذي يتعارض مع طبيعة الإنترنت وما تتميز به من سرعة، وهو الأمر الذي انعكس على الجرائم المتعلقة بالإنترنت (١٥). كذلك من الصعوبات الكبيرة في مجال المساعدات القضائية الدولية المتبادلة التباطؤ في الرد، حيث أن الدولة متلقية الطلب غالبا ما تكون متباطئة في الرد على الطلب سواء بسبب نقص الموظفين المدربين أو نتيجة الصعوبات اللغوية أو الفوارق في الإجراءات التي تعقد الاستجابة وغيرها من الأسباب (١٦).

ثانياً: التجريم المزدوج:

التجريم المزدوج من أهم الشروط الخاصة بنظام تسليم المجرمين، وبالرغم من أهميته، نجده.

١. عقبة أمام التعاون الدولي في مجال تسليم المجرمين بالنسبة للجرائم المعلوماتية سيما وأن معظم الدول لا تجرم هذه الجرائم.

٢. بالإضافة إلى أنه من الصعوبة أن نحدد فيما إذا كانت النصوص التقليدية لدى الدولة المطلوب منها التسليم يمكن أن تنطبق علي الجرائم المتعلقة بشبكة الإنترنت أولا. الأمر الذي يعوق تطبيق الاتفاقيات الدولية في مجال تسليم المجرمين، ويحول بالتالي دون جمع الأدلة ومحاكمة مرتكبي الجرائم المتعلقة بالإنترنت.

ثالثاً: عدم وجود نموذج موحد للنشاط الإجرامي.

ويقصد به أن يكون الفعل المطلوب التسليم من أجله مجرما في تشريع الدولة طالبة التسليم، وكذلك في تشريع الدولة المطلوب إليها التسليم. والمطلوب هنا أن يكون الفعل مجرما أيا كانت الصورة التشريعية المعاقب عليها فلا عبرة للوصف أو التكيف القانوني الذي يطلب على الفعل عند تقرير توافر هذه الشروط والمعاقبة عليه، فقد تختلف تشريعات الدول في التكيف القانوني الذي توصف فيه الجريمة فمثلا لو كان الفعل معاقبا عليه في تشريع الدولة الطالبة التسليم تحت مسمي جريمة توظيف الأموال، بينما كان الفعل نفسه معاقبا عليه تحت مسمي جريمة النصب والاحتيال في الدولة المطلوب منها التسليم فإن ذلك لا يمنع من توافر شرط ثنائية التجريم أو ازدواجيته (١٧). بنظرة للأنظمة القانونية القائمة في الكثير من الدول لمواجهة الجرائم المعلوماتية ومنها الجرائم المتعلقة بشبكة الإنترنت يتضح لنا من خلالها. عدم وجود اتفاق عام مشترك بين الدول حول نماذج إساءة استخدام نظم المعلومات وشبكة الإنترنت الواجب تجريمها، فما يكون مباحا في أحد الأنظمة قد يكون مجرما وغير مباح في نظام آخر ويمكن إرجاع ذلك إلى عدة أسباب وعوامل كاختلاف البيئات والعادات والتقاليد والديانات والثقافات من مجتمع لآخر، وبالتالي اختلاف السياسة التشريعية من مجتمع لآخر (١٨).

رابعاً: تنوع واختلاف النظم القانونية الإجرائية

١. بسبب تنوع واختلاف النظم القانونية الإجرائية، نجد أن طرق التحري والتحقيق والمحاكمة التي تثبت فائدتها وفاعليتها في دولة ما قد تكون عديمة الفائدة في دولة أخرى أو قد لا يسمح بإجرائها. كما هو الحال بالنسبة للمراقبة الإلكترونية، والتسليم المراقب، والعمليات المستترة، وغيرها من الإجراءات الشبيهة. فإذا ما اعتبرت طريقة ما من طرق جمع الاستدلالات أو التحقيق أنها قانونية في دولة معينة، قد تكون ذات الطريقة غير مشروعة في دولة أخرى (١٩). وبالتالي فإن الدولة الأولى سوف تشعر بخيبة أمل لعدم قدرة سلطات إنقاذ القانون في الدول الأخرى على استخدام ما تعتبره هي أنه أداة فعالة.

٢. بالإضافة إلى أن السلطات القضائية لدى الدولة الثانية قد لا تسمح باستخدام أي دليل إثبات جري جمعه بطرق تري هذه الدولة أنها طرق غير مشروعة، حتى وإن كان هذا الدليل تم الحصول عليه في اختصاص قضائي وبشكل مشروع (٢٠).

الفرع الثاني: صعوبات الاختصاص والتدريب وقنوات الاتصال التي تواجه الجهود الدولية

أولاً: مشكلة الاختصاص في الجرائم المتعلقة بالإنترنت:

الجرائم المتعلقة بالإنترنت من أكبر الجرائم التي تثير مسألة الاختصاص على المستوى المحلي أو الدولي ولا توجد أي مشكلة بالنسبة للاختصاص على المستوى الوطني أو المحلي حيث يتم الرجوع إلى المعايير المحددة قانونا لذلك.

ولكن المشكلة تثار بالنسبة للاختصاص على المستوى الدولي حيث اختلاف التشريعات والنظام القانونية والتي قد ينجم عنها تنازع في الاختصاص بين الدول بالنسبة للجرائم المتعلقة بالإنترنت التي تتميز بكونها عابرة للحدود. فقد يحدث أن ترتكب الجريمة في إقليم دولة معينة من قبل أجنبي، فهنا تكون الجريمة خاضعة للاختصاص الجنائي للدولة الأولى استنادا إلى مبدأ الإقليمية، وتخضع كذلك لاختصاص الدولة الثانية على أساس مبدأ الاختصاص الشخصي في جانبيه، وقد تكون هذه الجريمة من الجرائم التي تهدد أمن وسلامة دولة أخرى فتدخل عندئذ في اختصاصها استنادا إلي مبدأ العينية.

كما تثار فكرة تنازع الاختصاص القضائي في حالة تأسيس الاختصاص على مبدأ الإقليمية، كما لو قام الجاني بيث الصور الخليعة ذات الطابع الإباحي من إقليم دولة معينة وتم الاطلاع عليها في دولة أخرى، ففي هذه الحالة يثبت الاختصاص وفقا لمبدأ الإقليمية لكل دولة من الدول التي مستها الجريمة

ثانياً: الصعوبات التي تواجه الجهود الدولية في مجال التدريب [٢١].

١. تتمثل في عدم رغبة بعض القيادات الإدارية في بعض الدول في التدريب لاعتقادهم بدوره السلبي في تطوير العمل من خلال تطبيق ما تعلمه المتدربون في الدورات التدريبية وما اكتسبوه من خبرات..

٢. ومن الصعوبات أيضا والتي قد تهدد التعاون في مجال التدريب ما يتعلق بالفوارق الفردية بين المتدربين وتأثيرها على عملية الاكتساب للمهارات المستهدفة بقوة تامة ومتكافئة لدى مختلف الأفراد المتدربين.

٣. بالإضافة إلى أن نظرة المتدرب إلى الدورة التدريبية على أنها مرحلة تدريبية أو عبء لا طائل منه تهدد العملية التدريبية برمتها وبالطبع نسف التعاون الدولي في هذا المجال..

٤. أيضا من الصعوبات التي قد تؤثر على العملية التدريبية وعلى التعاون الدولي فيها ما يتعلق بالملامح العامة المميزة للبيئة التدريبية وعدم قدرتها على تمثيل الواقع العملي لبيئة العمل الطبيعة تمثيلا تاما ومتقنا، من حيث ما يدور بها من وقائع وملابسات وإجراءات، وما يتم فيها من نشاطات لا تبلغ حد التطابق مع طبيعة المهام التي سيؤديها المتدربون في بيئة العمل الطبيعية.

ثالثاً: الصعوبات التي تواجه الجهود الدولية في مجال قنوات اتصال.

أهم الأهداف المرجوة من الجهود الدولية في مجال الجريمة والمجرمين، الحصول على المعلومات والبيانات المتعلقة بهم، ولتحقيق هذا الهدف كان لزاما أن يكون هناك نظام اتصال يسمح للجهات القائمة على التحقيق بالاتصال بجهات أجنبية لجمع أدلة معينة أو معلومات مهمة [٢٢]، فعدم وجود مثل هذا النظام يعني عدم القدرة على جمع الأدلة والمعلومات العملية التي غالبا ما تكون مفيدة في التصدي لجرائم معينة ولمجرمين معينين. وبالتالي تنعدم الفائدة من هذا التعاون.

المطلب الثاني: كيفية القضاء على الصعوبات التي تواجه الجهود الدولية في مكافحة جرائم المعلوماتية

أولاً: حل العقبة المتعلقة بالمساعدات القضائية الدولية:

١. تبادل المعلومات: وهو يشمل تقديم المعلومات والبيانات والوثائق والمواد الاستدلالية التي تطلبها سلطة قضائية أجنبية وهي بصدد النظر في جريمة ما، عن الاتهامات التي وجهت إلى رعاياها في الخارج والإجراءات التي اتخذت ضدهم.

٢. نقل الإجراءات: ويقصد به قيام دولة ما بناء على اتفاقية أو معاهدة باتخاذ إجراءات جنائية وهي بصدد جريمة ارتكبت في إقليم دولة أخرى ولمصلحة هذه الدولة متى ما توافرت شروط معينة.

ثانياً: حل عقبة عدم وجود نموذج موحد للنشاط الإجرامي.

يتم حل هذه العقبة بتوحيد النظم القانونية. وتخفف من غلو الفوارق بين الأنظمة العقابية الداخلة، وذلك من خلال في تحديث التشريعات المحلية المعنية بالجرائم المعلوماتية وإبرام اتفاقيات خاصة يراعي فيها هذا النوع من الجرائم [٢٣].

ثالثاً: حل عقبة تنوع واختلاف النظم القانونية الإجرائية.

بالنسبة لمعوقة الخاصة بتنوع واختلاف النظم القانونية الإجرائية نجد أن الصكوك الدولية الصادرة عن الأمم المتحدة غالبا ما تشجع الأطراف فيها على السماح باستخدام بعض تقنيات التحقيق الخاصة، الشيء الذي يخفف من غلو واختلاف النظم القانونية والإجرائية ويفتح المجال أمام تعاون دولي فعال، فمثلا المادة (٢٠) من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية تشير في هذا الصدد إلى التسليم المراقب، والمراقبة الإلكترونية وغيرها من أشكال المراقبة والعمليات المستترة، و التي تعتبر من أهم التقنيات المستخدمة في التصدي للجماعات الإجرامية المنظمة المحنكة بسبب الأخطار والصعوبات الكامنة وراء محاولة الوصول إلى عملياتها وتجميع المعلومات وأدلة الإثبات لاستخدامها فيما بعد في الملاحقات القضائية المحلية منها أو الدولية في دول أطراف في سياق نظم المساعدة القانونية المتبادلة [٢٤].

وهذا ما أكدت عليه الاتفاقية الأوربية للإجرام المعلوماتي حيث نصت المادة ٢٩ على سرية حفظ البيانات المعلوماتية المخزنة وأجازت لكل طرف أن يطلب من الطرف الآخر الحفظ السريع للمعلومات المخزنة عن طريق إحدى الوسائل الإلكترونية الموجودة

داخل النطاق المكاني لذلك الطرف الآخر والتي ينوي الطرف طالب المساعدة أن يقدم طلباً للمساعدة بشأنها بغرض القيام بالتفتيش أو الدخول بأي طريقة مماثلة وضبط أو الحصول أو الكشف عن البيانات المشار إليها. كما أشارت المادة ٣١ إلى المساعدة المتعلقة بالدخول إلى البيانات المحفوظة، حيث أجازت لأي طرف أن يطلب من أي طرف آخر أن يقوم بالتفتيش أو أن يدخل بأي طريقة مشابهة وأن يضبط أو يحصل بطريقة مماثل وأن يكشف عن البيانات المحفوظة بواسطة شبكة المعلومات يضا نصت المادة ٣٣ على تعاون الدول الأطراف فيما بينها لجمع البيانات في الوقت الحقيقي عن التجارة غير المشروعة. ونلاحظ مما سبق أن الاتفاقية الأوربية للإجرام المعلوماتي أوجدت بعض الحلول التي من شأنها التغلب على مشكلة اختلاف النظم الإجرائية أمام التعاون الدولي لمواجهة الجرائم المتعلقة بشبكة الإنترنت.

رابعاً: حل عقبة عدم وجود قنوات اتصال.

للحد من ظاهرة عدم وجود قنوات اتصال بين جهات إنفاذ القانون فنلاحظ أنه غالبا ما تشجع الصكوك الدولية الدول إلى التعاون فيما بينها و تدعوها إلى إنشاء قنوات اتصال بين سلطاتها المختصة ووكالاتها ودوائرها المتخصصة بغية التيسير في الحصول علي هذه المعلومات وتبادلها [٢٥]، ومن الأمثلة على هذه الصكوك الدولية اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية والاتفاقية الأوربية التي أوجبت على الدول الأطرف فيها ضرورة تحديد نقطة اتصال تعمل لمدة ٢٤ ساعة يوميا طوال أيام الأسبوع لكي تؤمن المساعدة المباشرة للتحقيقات المتعلقة بجرائم البيانات والشبكات، أو استقبال الأدلة ذات الشكل الإلكتروني.

خامساً: حل عقبة الاختصاص في الجرائم الإنترنتية.

بالنسبة لمشكلة الاختصاص في الجرائم الإنترنتية فثمة حاجة ملحة إلى:

١. إبرام اتفاقيات دولية ثنائية كانت أو جماعية يتم فيها توحيد وجهات النظر فيما يتعلق بقواعد الاختصاص القضائي خاصة بالنسبة للجرائم المتعلقة بالإنترنت.

٢. بالإضافة إلى تحديث القوانين الجنائية الموضوعية منها والإجرائية بما يتناسب والتطور الكبير التي تشهده تكنولوجيا المعلومات والاتصالات.

سادساً: حل عقبة تواجه الجهود الدولية في مجال التدريب.

أما فيما يتعلق بالصعوبات التي تواجه الجهود الدولية في مجال التدريب فإنه يمكن التغلب عليها بإجراء المزيد من الحملات التوعوية للتنبيه بمخاطر الجرائم المعلوماتية والأضرار التي تسببها وبأهمية تدريب رجال العدالة الجزائية على مواجهتها، كما أنه وبمزيد من التنسيق بن الأجهزة المعنية بتدريب رجال تنفيذ القانون إيجاد برامج تدريبية مشتركة تناسب جميع الفئات. هذا بالإضافة إلى القيام ببعض العمليات المشتركة والتي من شأنها صقل مهارات القائمين على مكافحة تلك الجرائم وتقريب وجهات النظر بشأنها.

٨. خاتمة

يناقش هذا البحث واحدة من أهم القضايا التي تقلق رجال الفكر القانوني في الوقت الحاضر تلك هي الجريمة المعلوماتية. فأتساع استخدام الحاسوب وما تبعه من استخدام الشبكة الدولية وما نجم عنه من أنماط جديدة للسلوك الإجرامي لم يكن يتوقعه المشرع في معظم بلدان العالم الأمر الذي دفع بالدول إلى الوقوف وقفة جادة لمعالجة هذه المشكلة. وللوقوف على أهمية هذه المشكلة وأبعادها الدولية والإقليمية فقد جاء البحث في مبحثان تليهما الخاتمة وجملة من التوصيات.

يتناول البحث الأول الجهود الدولية والإقليمية لمكافحة جرائم المعلوماتية وفي إطار ثلاثة مطالب الأول ناقش الجهود الدولية لمكافحة جرائم المعلوماتية من خلال الاتفاقية الأوربية لمكافحة جرائم الإنترنيت اتفاقية بودابست/ ٢٠٠١. والاتفاقية الأمريكية المتعلقة بجرائم الحاسب الآلي والإنترنيت لسنة ١٩٩٩ فيما وضح المطلب الثاني الجهود الإقليمية لمكافحة جرائم المعلوماتية من خلال جهود الدول الأجنبية الأمريكية والبريطانية والفرنسية لمكافحة جرائم المعلوماتية، إلى جانب جهود الدول العربية المتمثل بالدول السعودية ودولة الأمارات العربية والأردن.

أما المبحث الثاني فقد تناول الصعوبات التي تواجه الجهود الدولي لمكافحة جرائم المعلوماتية وكيفية القضاء عليها في مطلبين تناول المطلب الأول الصعوبات التي تواجه الجهود الدولية لمكافحة جرائم المعلوماتية من خلال محورين المحور الأول تناول الصعوبات

التشريعية والقضائية التي تواجه الجهود الدولية والتجريم المزدوج وعدم وجود نموذج موحد للنشاط الإجرامي وتنوع واختلاف النظم القانونية الإجرائية أما المحور الثاني تناول صعوبات الاختصاص والتدريب وقنوات الاتصال التي تواجه التعاون الدولي ومشكلة الاختصاص في الجرائم المتعلقة بالإنترنت والصعوبات الخاصة بالجهود الدولية في مجال التدريب وعدم وجود قنوات اتصال وفي المطلب الثاني تناولنا كيفية القضاء علي الصعوبات التي تواجه الجهود الدولية في مكافحة جرائم المعلوماتية.

٩. النتائج

- إن تنامي ظاهرة الجرائم المعلوماتية عبر الوطنية، وتخطي آثارها حدود الدول، أفرز جملة من التحديات القانونية على الصعيد الإجرائي تجسدت في المقام الأول في بعض الصعوبات التي تكتنف إثبات هذه الجرائم وقبول الدليل بشأنها باعتبارها لا تترك أثراً مادياً ملموساً، كما هو الحال في الجرائم التقليدية.
- فضلاً عما يثيره ذلك من عقبات تواجه الأجهزة القضائية والأمنية في سبيل مباشرة بعض الإجراءات عبر الحدود كالمعاينة والتفتيش والضبط في نطاق البيئة الافتراضية. يضاف إلى هذا وذاك مشكلة تنازع الاختصاص بصدد هذه الجرائم باعتباره أن آثارها تتجاوز حدود الدول، الأمر الذي يجعل الحلول الوطنية غير مجدية، وتظل مشوبة بالقصور وعدم النجاعة.

١٠. التوصيات

توصلنا في هذه الدراسة إلى جملة من التوصيات، وهي على النحو التالي:

- نأمل أن تسعي الدول العربية إلى إنشاء منظمة عربية تهتم بالتنسيق في مجال مكافحة الجرائم المعلوماتية عبر الإنترنت؛ مع تشجيع قيام اتحادات عربية تهتم بالتصدي لجرائم الإنترنت وتفعيل دور المنظمات والإدارات والحكومات العربية في مواجهة هذه الجرائم عن طريقة نظام الأمن الوقائي.
- نأمل أن يتم التنسيق بين دول مجلس التعاون الخليجي بشأن مكافحة الجرائم المعلوماتية. سواء على مستوى الوقاية من هذه الجرائم؛ وسواء على مستوى ملاحقة الجناة والتحقيق معهم ومحاكمتهم.
- على الدول العربية المضي في عقد اتفاقات دولية إقليمية وعربية للتعاون على مكافحة الجرائم المعلوماتية على المستوى التشريعي والتنسيق فيما بينها لتعاون أجهزة الشرطة لتبادل البيانات والمعلومات، بل والمهارات اللازمة لملاحقة المتهمين بارتكاب الجريمة المعلوماتية.
- إنشاء مركز وطني مختص بجرائم تقنية المعلومات، يرمي لوضع برنامج شامل يهدف إلي التوعية المستدامة بالتشريعات والتطبيقات والتعاون بين مؤسسات المجتمع ككل وأفراده لمكافحة جرائم تقنية المعلومات.
- إجراء دراسات بحثية مسحية متخصصة بجرائم تقنية المعلومات، من قبل الأجهزة المعنية في الدولة، والتي تعبر عن كافة شرائح المجتمع، الأمر الذي يسمح بتوفير قاعدة معلومات صادقة تعكس الحالة الرقمية المجتمعية.
- الاستعانة بالتجارب الإقليمية والدولية في مكافحة جرائم تقنية المعلومات والاستفادة منها في استشراف العمليات الاحتيالية المختلفة، ووضع التدابير اللازمة لها.
- التأكيد على استمرارية عقد مثل هذه المؤتمرات المتخصصة والندوات وحلقات النقاش وورش العمل في مجال جرائم تقنية المعلومات خصوصاً ما يتعلق منها بجرائم الأدلة الرقمية والطلب الشرعي الإلكتروني، بما لها من آثار إيجابية للوقوف على أحدث العمل علي إعادة النظر في المناهج الدراسية في كليات القانون، وضرورة تضمينها مادة عامة عن الحاسب الآلي والشبكات المعلوماتية، بالإضافة إلى ضرورة إدراج الجانب المعلوماتي لكل مادة قانونية فيجب أن تتضمن الجرائم المعلوماتية مع القسم الخاص لمادة قانون العقوبات، وتدريس المحاكم الإلكترونية في مادة المرافعات وفي الختام أسال الله العلي القدير أن يوفقني بهذا العمل، وينفع به جميع الدول.

المراجع

[١] الشحات، حاتم عبد الرحمن، ٢٠٠٢، الإجرام المعلوماتي، دار النهضة العربية، القاهرة، ط١. بحث بعنوان التعاون الأمني الدولي في مكافحة الجريمة المنظمة، ص٣٦ منشور على الموقع الكتروني www.aim-council.org

[٢] عبد المجيد محمود، ٢٠٠٥، الآلية تنفيذ اتفاقية الأمم المتحدة لمكافحة الفساد، بحث مقدم إلى ندوه "حول اتفاقية الأمم المتحدة لمكافحة الفساد" ١٥ – ١٦ حزيدان/ يونيه – القاهرة.

[٣] عباينة، محمود أحمد، ٢٠٠٤، جرائم الحاسوب وإبعادها الدولية، دار الثقافة والنشر والتوزيع.

[٤]Computer Hackers: Tomorrows Tarrarts Dynamics, News for and about members of the American society for in dustrial seturdy jam varyl febrauary. ١٩٩٠

[٥] قشقوش، هدي حامد، ١٩٩٢، "جرائم الحاسب الإلكتروني". دار النهضة العربية، طبعة ١٩٩٢، ص٦٦.

[٦] النبهان، محمد فاروق، ١٩٩٢، نحو استراتيجية عربية موحدة لمكافحة الإجرام المنظم، دار الجامعة، ط١. ١٩٩٢، ص١٩٣

[٧] قشقوش، هدي حامد، ١٩٩٢، "جرائم الحاسب الإلكتروني، المرجع السابق ص ٦٦.

[٨] الملط، أحمد خليفة، ٢٠٠١ الجرائم المعلوماتية، دار الفكر العربي، الإسكندرية، ص٤٤.

[٩] التجارة الإلكترونية في المملكة انطلاقاً نحو المستقبل، وزارة التجارة، ١٤٢٣هـ.

[١٠] الشافعي، محمد إبراهيم محمد، ٢٠٠٤، النقود الإلكترونية، مجلة الأمن والحياة، أكاديمية الشرطة، دبي س١٢، ع١، يناير.

[١١] نضال يوسف إيليا، بحث بعنوان دور المجتمع العراقي في مكافحة جرائم الكمبيوتر والإنترنيت، مقدم إلى ندوة علمية بعنوان واقع خدمة الإنترنيت وانعكاسها على المستهلك العراقي جامعة بغداد. ص٩.

[١٢] السالمي، علاء عبد الرزاق، ٢٠٠٢، تكنولوجيا المعلومات، دار المناهج للنشر والتوزيع، عمان، الأردن.

[١٣] الأوجلي، سالم، أحكام المسئولية الجنائية عن الجرائم الدولية، رسالة دكتوراه، كلية الحقوق جامعة عين شمس ١٩٩٧م.

[١٤] حسين، محمد عبد الطاهر، ٢٠٠٢، المسئولية القانونية في مجال شبكات الإنترنت، دار النهضة العربية القاهرة.

[١٥] الشافعي، محمد إبراهيم محمد، ٢٠٠٤، النقود الإلكترونية، مجلة الأمن والحياة، أكاديمية الشرطة، دبي، س١٢، ع١، يناير، ص٢٢.

[١٦] الروبي، سراج الدين محمد، ١٩٩٨م، الإنتربول وملاحقة المجرمين، الدار المصرية اللبنانية ص٥٣.

[١٧] الصغير، جمال عبد الباقي، ١٩٩٢، القانون الجنائي والتكنولوجيا الحديثة، دار النهضة العربية القاهرة.

[١٨] Computer Hackers: Tomorrows Tarrarts Dynamics,.Cit. p:٢٢.

[١٩] الشافعي، محمد إبراهيم محمد، ٢٠٠٤، النقود الإلكترونية،، مرجع سابق، ص٢٢.

[٢٠] الشهري فايز بن عبد الله التحديات الأمنية المصاحبة لوسائل الاتصال الجديدة دراسة وصفية تأصيلية للظاهرة الإجرامية على شبكة الإنترنيت، الدليل الإلكتروني للقانون العربي arablawinfe

[٢١] الصغير، جمال عبد الباقي، الجوانب الإجرائي، المرجع السابق ص ٧٤.

[٢٢] الرومي، محمد أمين، ٢٠٠٣، جرائم الكمبيوتر والإنترنيت، دار المطبوعات الجامعية، ط١، ص١٠٢.

[٢٣] منشورات الأمم المتحدة رقم المبيع (E.O.٥.V٢) الجزء الأول – الفقرة ٣٨٤.

[٢٤] ما جاء بتوصية المجلس الأوربي رقم ١٣ (R٩٥) الصادرة في ١١/ ٠٩/ ١٩٩٩ بشأن مشاكل الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات

[٢٥] السالمي، علاء عبد الرزاق، ٢٠٠٢، تكنولوجيا المعلومات، المرجع السابق، ص١٢١.